Réaliser un audit des comptes utilisateurs avec des droits administratifs dans un domaine Active Directory en mode mixte:

Historique des modifications :			
Version	Date	Origine mise à jour :	Rédigé par :
1.0	10/07/07	Version initiale	Guillaume MATHIEU

I. INTRODUCTION : 3

A. OBJECTIF DE CE DOSSIER : 3
B. ARCHITECTURE DE TEST : 3
C. OU TELECHARGER CE DOCUMENT ET LE SCRIPT ASSOCIE : 3

II. OBJECTIFS DU SCRIPT : 4

III. ANALYSE DU FONCTIONNEMENT DU SCRIPT : 5

A. QUELQUES PRECISIONS SUR LES ATTRIBUTS LASTLOGON ET LASTLOGON TIMESTAMP DE L'ANNUAIRE (POUR UN OBJET COMPTE UTILISATEUR) : 5
B. LES DIFFERENTES PHASES DU SCRIPT : 5
1. Etape 1 : établir la liste des contrôleurs de domaine : 5
2. Etape 2 : lister les utilisateurs membres des groupes à auditer et récupérer les informations sur les comptes utilisateurs (nom, date de dernier login, statut…) : 6
3. Etape 3 : mise à jour de la date de dernier login : 6
4. Etape 4 : le script affichera le tableau sous forme de fichier CSV : 6

IV. MODE D'EMPLOI DU SCRIPT : 7

A. ETAPE 1 : DECLARATION DE LA DIMENSION DU TABLEAU DE RESULTAT 7
B. ETAPE 2 : DECLARER LES CONTROLEURS DE DOMAINE A AUDITER : 7
C. ETAPE 3 : DEFINIR LE SEPARATEUR POUR LE FICHIER DE SORTIE : 7
D. ETAPE 4 : DEFINIR LA DATE LIMITE : 7
E. ETAPE 5: DEFINIR LE CHEMIN LDAP DES COMPTES A AUDITER : 7
F. ETAPE 6 : EXECUTION DU SCRIPT 8
G. ETAPE 7 : TRAITEMENT DU FICHIER DE SORTIE : 8
H. TESTS DU SCRIPT ET RESULTAT : 8
1. L'architecture de tests : 8
2. Résultats : 8
3. Interprétation des résultats : 8

I. Introduction :

A. Objectif de ce dossier :

Le principal objectif de ce document est de vous présenter une solution clé en main que j'ai déployé chez un de mes clients pour auditer les comptes utilisateurs membres des groupes suivants :

- Builtin\Administrateurs
- Builtin\Opérateurs de Compte
- Builtin\Opérateurs de Sauvegarde
- Admins du domaine

Le but dans un premier temps est de déterminer quel est le rôle de chaque compte et s'il est toujours utilisé. Ces informations doivent être consolidé dans un fichier Excel et le tout automatiquement (écriture d'un script au format vbscript).

B. Architecture de test :

Nous nous baserons dans ce dossier sur l'architecture suivante :

- Un domaine Active Directory en mode mixte.
- 15 contrôleurs de domaine dont 5 contrôleurs de domaine Windows 2003 Server et 10 BDC NT4 sp6.

C. Où télécharger ce document et le script associé :

Ce document peut être télécharger au format PDF à l'adresse suivante :
http://msreport.free.fr/articles/audit_securite.pdf
Le script peut être télécharger à l'adresse suivante :
http://msreport.free.fr/articles/audit_securite.vbs

II. Objectifs du script :

Le script a pour but de :

- Lister les utilisateurs qui sont membres des groupes « Admins du domaine », « Built-in\Administrateurs », « Built-in\Opérateurs de sauvegardes », « Built-in\Opérateurs de Compte».
- Comprendre à quoi servent les comptes utilisateurs qui sont membres de ces groupes.
- Déterminer quels sont les comptes utilisateurs qui ne se sont pas logués depuis 60 jours (ou autre date limite)
- Déterminer quels sont les comptes qui sont déjà désactivés.
- Consolider ces informations dans un fichier Excel (génération automatique).

III. Analyse du fonctionnement du script :

A. Quelques précisions sur les attributs lastLogon et lastLogon Timestamp de l'annuaire (pour un objet compte utilisateur) :

Il existe 2 attributs pour un objet compte utilisateur qui permettent de déterminer quand un utilisateur s'est connecté à un domaine Active Directory pour la dernière fois :

- L'attribut « lastLogon » : il contient la date de dernier login sur un contrôleur de domaine particulier. Cet attribut n'étant pas répliqué sur tous les contrôleurs de domaine, il est nécessaire d'interroger tous les contrôleurs de domaine pour connaître la date de dernier login d'un compte utilisateur. Cette date est en fait un compteur qui s'incrémente de 1 toutes les 100 nanosecondes et qui prend comme date de départ le 01 janvier 1601 à 00h00.
- L'attribut « lastLogonTimestamp » : il est sur le même principe que l'attribut « lastLogon » sauf qu'il est répliqué sur tous les contrôleurs de domaine une fois tous les 14 jours. Pour bénéficier de cet attribut, il faut être en mode de domaine Fonctionnalité 2003 (natif 2003). Pour plus d'informations, voir http://www.microsoft.com/technet/prodtechnol/windowsserver2003/fr/library/ServerHelp/91a98c38-38c5-49dc-83bf-e69d8e1dbbfa.mspx?mfr=true

Comme nous sommes en mode natif, nous allons donc utiliser l'attribut lastLogon ce qui nous obligera éventuellement à interroger les autres contrôleurs de domaine.

B. Les différentes phases du script :

Le script va nous permettre de récupérer automatiquement la liste des comptes utilisateurs membres des groupes « Admins du domaine », « Built-in\Opérateurs de Compte», « Built-in\Opérateurs de sauvegardes » et « Built-in\Administrateurs ».
Pour chaque compte utilisateur nous allons ensuite récupérer les informations suivantes :

- Login du compte utilisateur
- Description du compte utilisateur
- Date de dernier login du compte
- Etat du compte (activé ou non)
- Chemin LDAP du compte.

Ce script se découpe en 4 étapes.

1. Etape 1 : établir la liste des contrôleurs de domaine :

Avant d'exécuter le script, il est nécessaire d'établir la liste des contrôleurs de domaine 2003 et des BDC NT4. Il est important de placer en tête de liste, les contrôleurs de domaine sur lesquels les comptes utilisateurs avec privilèges sont censés s'être logués.
En effet, l'analyse de la date de dernier login s'arrêtera dès que le script aura identifié un contrôleur de domaine avec lequel le compte utilisateur a ouvert une session depuis moins de 60 jours. Cela permettra de prouver que le compte utilisateur est toujours utilisé et ne doit donc pas être désactivé sans raison. Ces informations seront renseignées en dur dans le script.

2. Etape 2 : lister les utilisateurs membres des groupes à auditer et récupérer les informations sur les comptes utilisateurs (nom, date de dernier login, statut…) :

Le script interrogera le premier contrôleur de domaine 2003. Il permettra de créer une matrice (tableau à 2 dimensions) qui stockera les informations de chaque compte utilisateur.
Les informations contenues dans cette matrice seront alors complète mis à part pour la date de dernier logon.

3. Etape 3 : mise à jour de la date de dernier login :

Si la date de dernier login d'un compte dans la matrice (tableau de résultat) est inexistante ou antérieure à la date limite, le script se connectera aux autres contrôleurs de domaine (selon un ordre définis à l'étape 1) pour essayer de mettre à jour cette information. Le script s'arrêtera dès qu'une date de dernier login plus récente que la date limite aura été trouvé sur un autre contrôleur de domaine.

4. Etape 4 : le script affichera le tableau sous forme de fichier CSV :

Le script affichera la matrice sous forme d'un fichier au format CSV.

IV. Mode d'emploi du script :

A. Etape 1 : Déclaration de la dimension du tableau de résultat

Chaque compte utilisateur listé comme appartenant au moins à 1 des 4 groupes que l'on audite va être référencer dans une matrice appelée « Resu ». C'est cette matrice que l'on affichera dans la phase 4 du script.
La première dimension permet de différencier les comptes utilisateurs. La seconde dimension permet d'accéder aux propriétés de chaque compte utilisateur.
Si vous pensez que vous disposez d'environ 1000 comptes, déclarer la matrice ainsi :
Resu [1500,15]
On a ainsi une marge d'environ 500 comptes utilisateurs avant de saturer le tableau.

B. Etape 2 : Déclarer les contrôleurs de domaine à auditer :

Il faut déclarer ensuite tous les contrôleurs de domaine sur lequel on va effectuer une analyse. Il est judicieux de mettre comme premier contrôleur de domaine de la liste, un serveur utilisé par le personnel informatique.
Attention le script est prévu pour commencer l'analyse sur les contrôleuses de domaine 2003. Une fois que l'analyse a été effectuée sur les DC 2003, il est possible de lancer l'analyse sur les BDC NT4.
Il est nécessaire de mettre à jour les variables suivantes :
nbdc2003 : indique le nombre de DC 2003 à analyser. Si vos avez déclarer 2 contrôleurs de domaine, nbdc2003 est égale à 2.
Nbbdc : indique le nombre de BDC NT4.

Si vous ne souhaitez faire l'analyse que sur des DC 2003 :

- bdc =0
- Supprimer le code de l'étape 3.2. (code entre les commentaires)

Si vous souhaitez faire l'analyse que sur des BDC NT4

- dc2003=0
- Supprimer le code de l'étape 3.1 (code entre les commentaires)

C. Etape 3 : Définir le séparateur pour le fichier de sortie :

Le script est configuré par défaut pour utiliser le « ; » comme séparateur.
Si votre tableur utilise la virgule comme caractère de séparation, modifier la valeur de la variable « separateur_csv ».

D. Etape 4 : définir la date limite :

Pour cela, changer la date de la variable « A ». Conserver le format de cette variable.

E. Etape 5: définir le chemin LDAP des comptes à auditer :

Il est nécessaire d'indiquer le chemin LDAP des groupes à auditer.
Le script est configuré pour auditer 4 groupes. Si vous souhaitez ajouter un cinquième groupe à auditer, copier la partie 2.2 du script.
La deuxième dimension de la matrice « Resu » servant à stocker les propriétés du compte, vous pouvez définir une nouvelle propriété. Attention les propriétés numérotées 1 à 10 sont déjà prises.
Dans la partie 4, modifier la sortie, pour qu'il ajoute une colonne dans le fichier de sortie.

F. Etape 6 : exécution du script

Ce script toi être exécuté sur un serveur 2003, de préférence le premier contrôleur de domaine de la liste des DC 2003.
Aller dans le menu démarrer et cliquer sur « Exécuter ».
Taper « cmd » et cliquer sur « Ok ».
Taper « cscript + le chemin du script et rediriger la sortie vers un fichier au format csv ».

G. Etape 7 : Traitement du fichier de sortie :

Ouvrir le fichier csv avec Excel.
Pour faciliter l'analyse, vous pouvez activer les filtres. Pour cela dans Excel 2003, aller dans le menu Données | Filtrer | Activer les filtres.
Vous pouvez aussi mettre en place des codes de couleur à l'aide des formats conditionnels. Pour cela, dans Excel 2003, sélectionner la colonne et aller, menu Format | Mise en forme conditionnelle.

H. Tests du script et résultat :

1. L'architecture de tests :

Domaine irs.com
2 contrôleurs de domaine 2003

- Dca.irs.com
- Dcb.irs.com

2 BDC NT4 :

- bdc1.irs.com
- bdc2.irs.com :

2. Résultats :

Il faut environ 10 minutes pour exécuter le script sur cette architecture de tests.
Le processeur est environ à 50% de charge pour le processus « cscript ».
La phase 2 prend environ 30 secondes. Ce sont les requêtes sur les autres DC qui prennent du temps
La bande passante utilisée est environ 2% sur un réseau 100 Mégabit.

3. Interprétation des résultats :

Pour des raisons de performance, privilégier l'exécution de ce script en soirée
L'arrêt de ce script via CTRL C va entraîner automatiquement l'arrêt des requêtes. Il est donc peu probable que ce script écroule le réseau malgré le nombre important de requête sur les contrôleurs de domaine.
Il faudra vérifier que les BDC NT4 peuvent être résolus depuis le serveur qui exécutera le script. En effet si le serveur n'est pas en ligne ou ne peut pas être résolu, on a un timeout de 20 secondes pour chaque requête.
Comme nous sommes en mode mixte, le groupe Admins du domaine ne peut contenir que des utilisateurs et pas d'autres groupes. Ce n'est pas le cas des groupes Builtin qui peuvent contenir d'autres groupes (comme Builtin\Administrateurs). Le groupe « Admins du domaine » apparaîtra entre autre donc dans le fichier résultat et sera à ignorer. Cela n'entraîne pas de problème au niveau du script.

Dans certains cas, il sera nécessaire de collecter des informations auprès du personnel informatique. Il est conseillé ensuite de mettre à jour le champ Description du compte utilisateur en question.